



Kit Izenpe

Instalación y manual de Usuario para Windows





Sumario

Introducción 3

A quién va dirigido este documento 3

Antes de comenzar 3

Instalación 4

Instalación desatendida (para usuarios avanzados) 7

Problemas durante la instalación 8

Fin de la instalación 8

Antes de comenzar a usar el Kit Izenpe 9

Acceso a la aplicación 9

Funcionalidades 11

Tabla de funciones 11

Preguntas frecuentes 14

Glosario 17

Introducción

Este manual sirve de guía para llevar a cabo de manera exitosa el proceso de instalación del Kit Izenpe, para el uso de las tarjetas criptográficas Izenpe (también para aquellas que vengan incorporadas en el token USB cryptoKEY), y el procedimiento para acceder y usar la aplicación de gestión. El Kit Izenpe consta de los siguientes componentes:

- **Izenpe Middleware**: librerías que permiten a cualquier aplicación del Sistema Operativo operar con las tarjetas criptográficas mencionadas
- **Izenpe Middleware para Citrix**: librería que permiten a cualquier aplicación Citrix operar con las tarjetas criptográficas mencionadas **(sólo se debe instalar cuando se trabaja bajo entornos Citrix)**
- **Izenpe Card Manager**: aplicación para la gestión de la tarjeta, que permite realizar operaciones como cambio de PIN o PUK, desbloqueo de PIN, obtener información sobre la tarjeta,…
- **Izenpe CertExpire**: aplicación de alerta de caducidad de certificados. Alerta de la próxima caducidad o de la ya caducidad de los certificados de las tarjetas inteligentes reconocidas por el Sistema Operativo
- **Controladores token cryptoKEY**: librerías para permitir al sistema operativo interactuar satisfactoriamente con el token USB cryptoKEY **(sólo en el caso que su tarjeta venga incorporada en un token USB cryptoKEY)**

Este manual le guiará de una manera sencilla en el proceso de instalación y uso del Kit Izenpe.

A quién va dirigido este documento

- ***Usuarios finales***, que van utilizar la tarjeta con chip de Izenpe.

Antes de comenzar

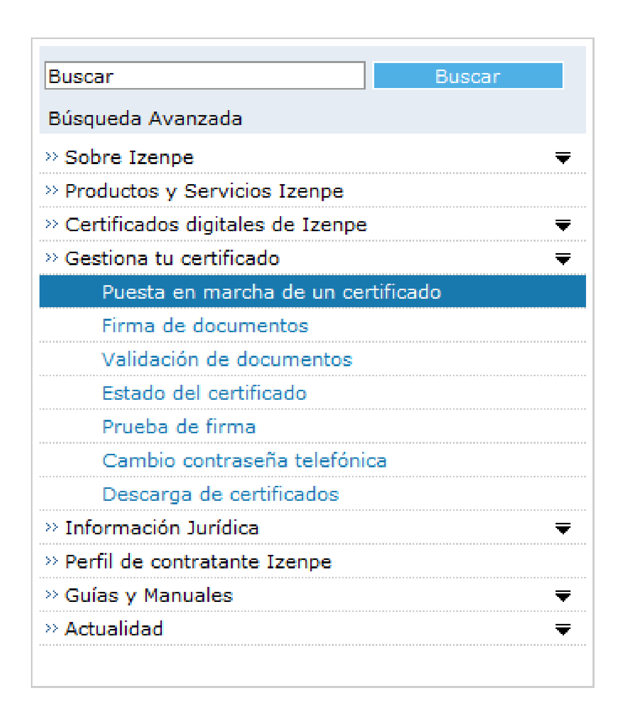
Asegúrese de disponer de:

- Un lector de tarjetas estándar, compatible PC/SC que se encuentre correctamente conectado, instalado y configurado. Siga las instrucciones suministradas por el fabricante del lector para verificar su correcta instalación y funcionamiento **(en el caso de disponer de un token cryptoKEY no es necesario).**
- Disponer de la última versión del Kit Izenpe. Recomendamos visitar el sitio web de Izenpe para verificar que se trata de la versión actualizada.
- Para poder realizar la instalación, es indispensable poseer permisos de Administrador. En caso de no poseerlos la instalación será denegada.

En el caso de disponer de un token USB cryptoKEY de Bit4id no lo conecte a su ordenador hasta que no haya concluido la instalación.

Instalación

La aplicación estará accesible a través de la web de Izenpe, a través del apartado "Gestiona tu certificado" > Puesta en marcha de un Certificado



Descargue el instalador correspondiente a Windows, y ejecútelo en su equipo. Si se le solicita, permita la ejecución de la aplicación.

Nota: En el caso de que no le solicite la ejecución de la aplicación vaya a la carpeta de descargas, busque el icono de Kit_Izenpe_User y ejecútelo desde allí.

Selección del idioma

Una vez ejecutada la aplicación se solicita al usuario la selección del idioma en el que se va a instalar la aplicación. Idiomas disponibles:

- Español
- Euskera
- Inglés



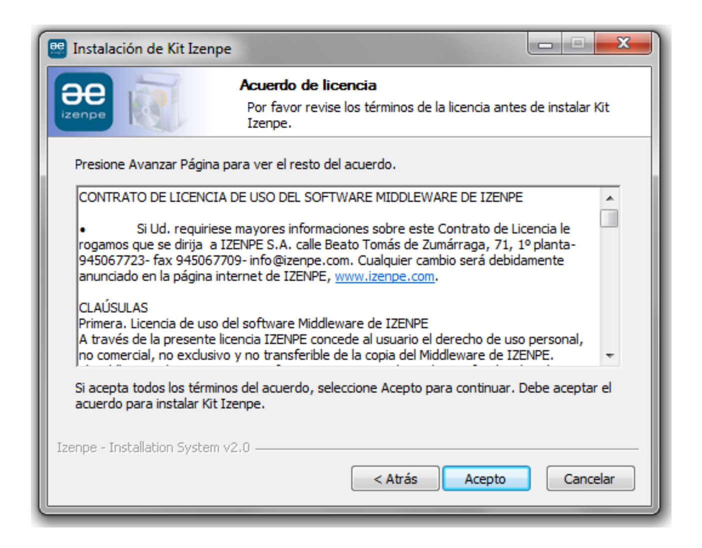
Seleccione el idioma y pulse OK. Se iniciará el Asistente de instalación que le guiará en el proceso. **Se recomienda cerrar cualquier otra aplicación antes de continuar con el proceso de instalación.**

Asistente de instalación

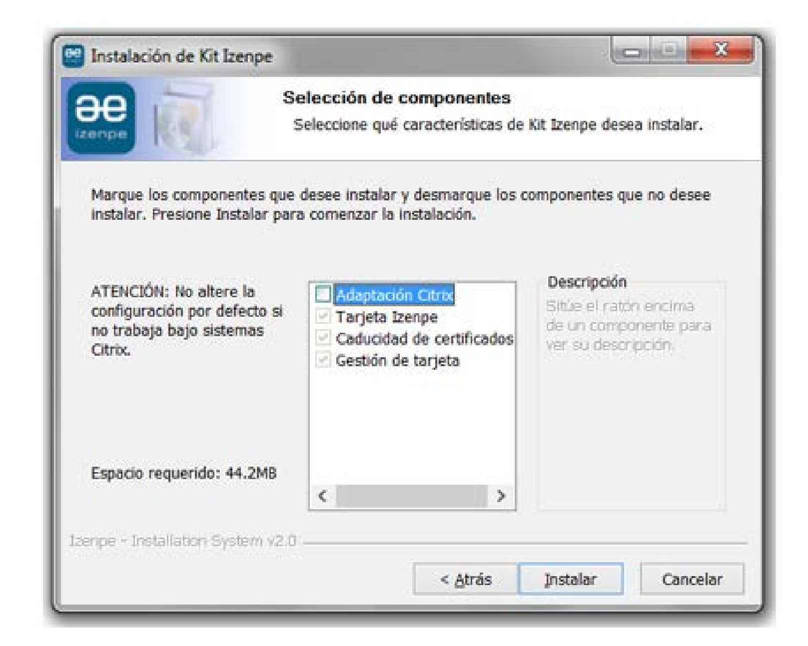
Bienvenido al Asistente de Instalación de Kit Izenpe. Haga click en *Siguiente* para continuar.



Revise los términos del acuerdo de licencia y haga click en *Acepto* para continuar



A continuación, se le mostrará una ventana con una lista seleccionable de todos los componentes a instalar. Los componentes obligatorios aparecerán con las casillas deshabilitadas. Mantenga la configuración por defecto y pulse *Instalar*.



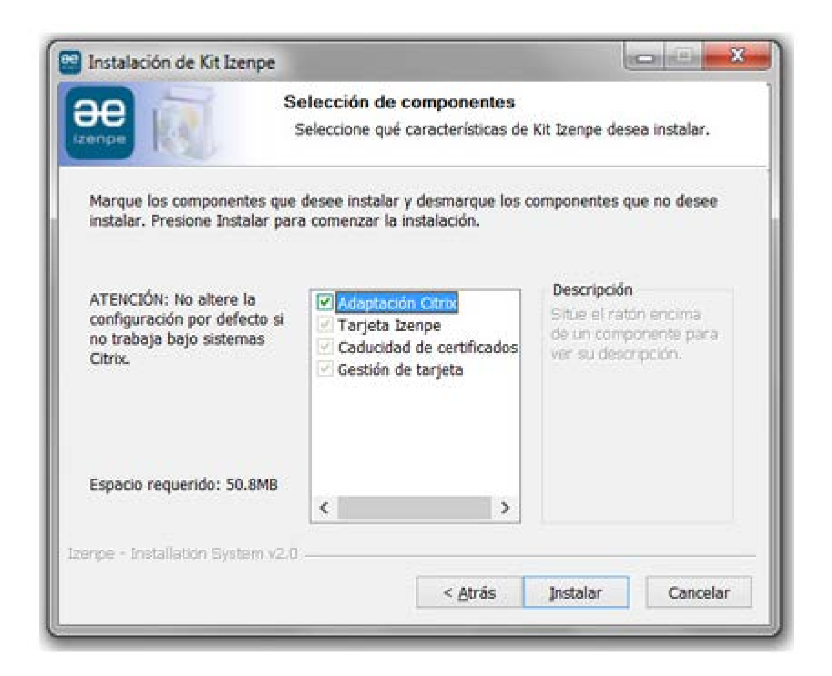
ATENCIÓN: No altere la configuración por defecto si no se lo especifica Izenpe pues podría provocar errores técnicos al trabajar con la tarjeta inteligente.

Presione *Terminar* para cerrar el asistente



Instalación avanzada (entornos Citrix)

Para la instalación del kit Izenpe bajo sistemas Citrix se requiere seleccionar el componente *Adaptación Citrix* en la lista de componentes que muestra en el asistente de instalación.



Instalación desatendida (para usuarios avanzados)

ATENCIÓN: este procedimiento es sólo para casos concretos en los que Izenpe se lo indique explícitamente. La mayoría de usuarios no deberían realizar una instalación desatendida.

Para poder realizar una instalación desatendida basta con introducir en el cuadro de comandos el instalador pasándole como parámetro "/S".

ATENCIÓN: debido a las limitaciones de interacción de una instalación desatendida, es necesario eliminar versiones anteriores o incompatibles (SafeSign) antes de proceder. Así mismo, se debe forzar el reinicio de la máquina una vez concluida la instalación.

Para la instalación desatendida en entornos Citrix se debe pasar además de *"/S"* el parámetro *"/C"*. El orden de los parámetro es indiferentes (*"/S /C"* o *"/C /S"*).

/S: indica instalación desatendida

/C: indica instalación adaptada para entornos Citrix

Ejemplos de instalación desatendida

- Instalación desatendida

Ruta del ejecutable> ***Kit_Izenpe_Admin_X.X.X.X /S***

Ruta del ejecutable> ***Kit_Izenpe_User_X.X.X.X /S***

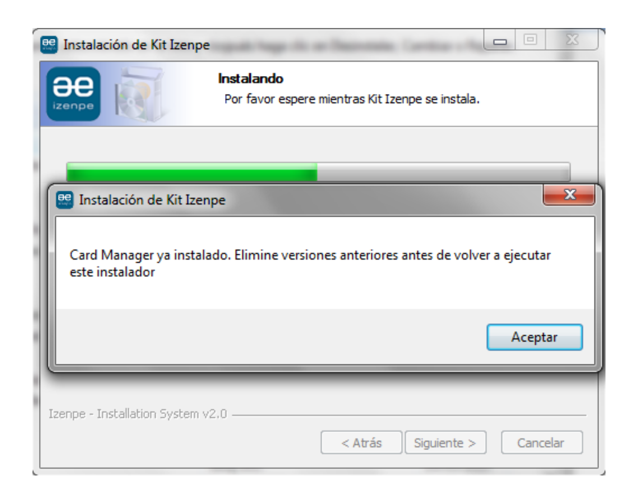
- Instalación desatendida para entornos Citrix

Ruta del ejecutable> ***Kit_Izenpe_User_X.X.X.X /S /C***

Ruta del ejecutable> ***Kit_Izenpe_Admin_X.X.X.X /C /S***

Problemas durante la instalación

Es posible que tenga versiones anteriores de la aplicación de Gestión de la tarjeta (Izenpe Card Manager) instaladas en su equipo, por lo que se le solicitará que elimine versiones anteriores antes de ejecutar el instalador. Elimine dichas versiones y ejecute de nuevo el instalador.



Para eliminar versiones anteriores en Windows XP, diríjase al menú Inicio > Programas > Izenpe > Desinstalar Kit Izenpe x.x.x.x (dónde x.x.x.x representa el número de versión instalada)

En el caso de Windows 8, para eliminar versiones anteriores, diríjase a la pantalla de Inicio y haga click con el botón derecho. Le aparecerá un icono con el nombre "Todas las aplicaciones". Púlselo y busque la aplicación de Izenpe > Desinstalar Kit Izenpe x.x.x.x (dónde x.x.x.x representa el número de versión instalada).

Fin de la instalación

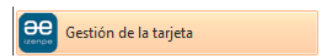
Una vez finalizado el proceso de instalación se creará un acceso directo en el escritorio de la aplicación Izenpe Card Manager (Gestión de la tarjeta) que le permitirá realizar cualquier tipo de operación con la misma.



Así mismo se puede acceder a la aplicación Gestión de Tarjeta a través de:

- en Windows XP, diríjase al menú Inicio > Programas > Izenpe > Gestión de la Tarjeta
- en Windows Vista o 7, diríjase al menú Inicio > Todos los programas > Izenpe > Gestión de la Tarjeta

- en Windows 8, diríjase a la pantalla de Inicio > Todas las aplicaciones > Izenpe > Gestión de la Tarjeta



En este momento puede conectar su token cryptoKEY de Bit4id a un puerto USB libre de su ordenador. Windows lo reconocerá automáticamente. El LED verde del dispositivo quedará fijo, indicando que la comunicación entre el token y el ordenador es satisfactoria, y todo funciona correctamente.

Antes de comenzar a usar el Kit Izenpe

Izenpe Card Manager requiere un lector de tarjetas inteligentes estándar, compatible PC/SC, que se encuentre correctamente conectado, instalado y configurado antes de comenzar.

Siga las instrucciones suministradas por el fabricante del lector para verificar su correcta instalación y funcionamiento.

En el caso de disponer de un token cryptoKEY asegúrese de tenerlo conectado a un puerto USB libre de su ordenador, y de que el token tiene una tarjeta inteligente (tamaño SIM) en su interior.



Acceso a la aplicación

La aplicación Izenpe Card Manager es accesible desde el escritorio, haciendo click sobre:



Así mismo recordamos que se puede acceder a la aplicación Gestión de Tarjeta a través de:

- en Windows XP, diríjase al menú Inicio > Programas > Izenpe > Gestión de la Tarjeta
- en Windows Vista o 7, diríjase al menú Inicio > Todos los programas > Izenpe > Gestión de la Tarjeta

- en Windows 8, diríjase a la pantalla de Inicio > Todas las aplicaciones > Izenpe > Gestión de la Tarjeta

Funcionalidades

Izenpe Card Manager (Gestión de la tarjeta) dispone de múltiples funcionalidades, accesibles desde la pantalla principal:



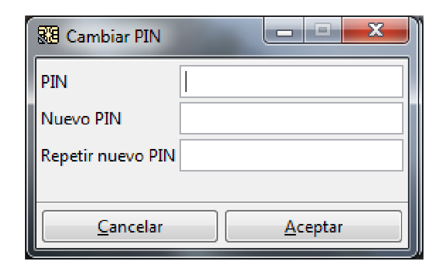
Tabla de funciones

La siguiente tabla resume las funciones expuestas en la pantalla principal de Izenpe Card Manager.

Función	Descripción
Cambiar PIN	Función para cambiar el PIN de la tarjeta (ver imagen 2)
Cambiar PUK	Función para cambiar el PUK de la tarjeta (ver imagen 2B)
Desbloquear PIN	Función para desbloquear el PIN de la tarjeta mediante el PUK de la misma (ver imagen 3)
Ver…	Función para ver el listado de certificados que se encuentra en la tarjeta (ver imagen 4)
Acerca de…	Función que muestra la versión instalada (ver imagen 5)
Seleccionar Lector	Función para seleccionar el lector con el que se quiere interactuar en el caso de que haya más de uno

Cambiar PIN

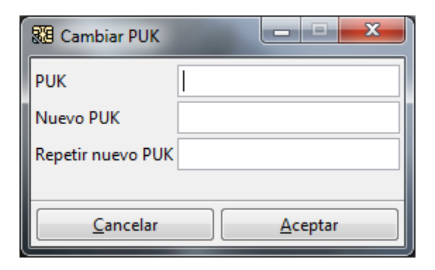
Introduzca el PIN antiguo de la tarjeta y el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.



[Imagen 2]

Cambiar PUK

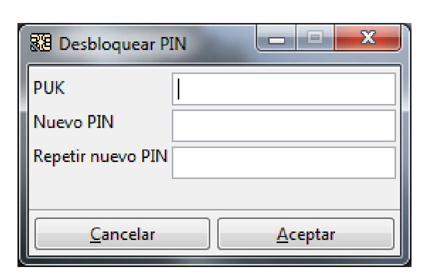
Introduzca el PUK antiguo de la tarjeta y el nuevo PUK. El nuevo PUK tiene que tener entre 6 y 8 dígitos alfanuméricos.



[Imagen 2B]

Desbloquear PIN

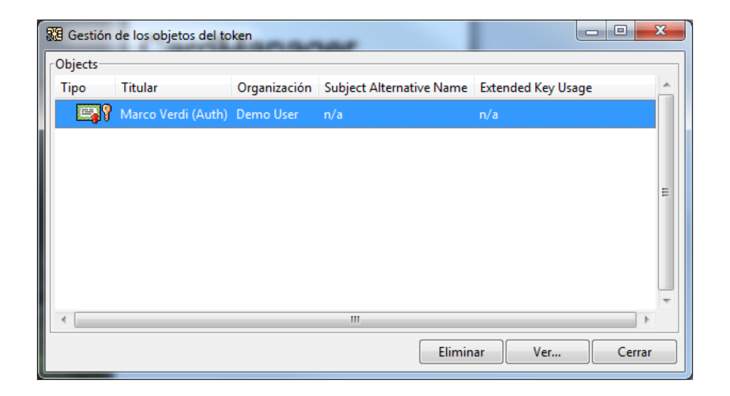
Para desbloquear el PIN, introduzca el PUK de la tarjeta e introducir el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.



[Imagen 3]

Ver…

Para ver los certificados que se encuentran en la tarjeta, introduzca el PIN de la tarjeta cuando sea solicitado.



[Imagen 4]

Acerca de…

Ventana que muestra la versión del Kit Izenpe, que le puede solicitar el CAU.



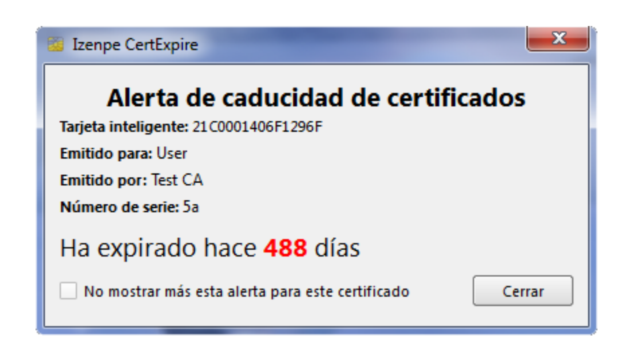
[Imagen 5]

Alerta de certificados

Cuando inserte la tarjeta inteligente en el lector con algún certificado caducado o próximo a caduca (de validez inferior o igual a 30 días) la aplicación le alertará a través de una ventana emergente:

Certificado caducado

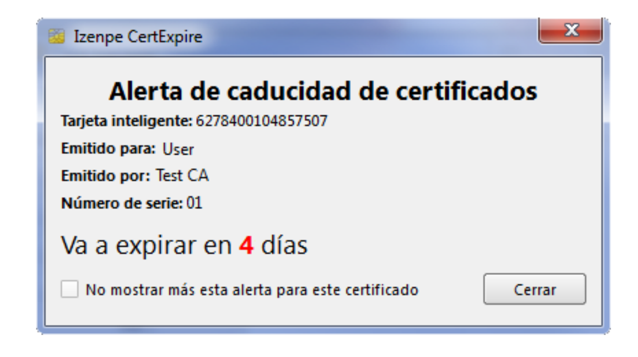
Se le mostrará una ventana emergente como la de la imagen 9. En ella se le mostrarán varios valores referentes al certificado y a la tarjeta inteligente donde se aloja el mismo. Además, se le mostrará de manera destacada los días que han pasado desde la expiración del mismo (*Ha expirado hace X días*).



[Imagen 9]

Certificado próximo a caducar

Se le mostrará una ventana emergente como la de la imagen 10. En ella se le mostrarán varios valores referentes al certificado y a la tarjeta inteligente donde se aloja el mismo. Además, se le mostrará de manera destacada los días que han pasado desde la expiración del mismo (*Va a expirar en X días*).



[Imagen 10]

Evitar futuras alertas

Los mensajes de alerta aparecerán cada vez que se inserte la tarjeta. En ambos casos, caducidad o pronta caducidad del certificado, se puede evitar la muestra de la ventana emergente seleccionando la casilla "*No mostrar más esta alerta para este certificado*".

Preguntas frecuentes

¿Qué puede ocurrir si, usando Card Manager, me aparece el mensaje de error "C_OpenSession debido al error 0x1"?

Consulte con Izenpe sobre el estado de la tarjeta, indicando todos los pasos que ha llevado a cabo.

¿Qué puede ocurrir si, usando Card Manager, me aparece el mensaje de error "C_Login debido al error 0x5"?

Es posible que el código PIN de su tarjeta se encuentre en un estado inconsistente. Pruebe a cambiarlo.

Si el error permanece, consulte con Izenpe sobre el estado de la tarjeta, indicando todos los pasos que ha llevado a cabo.

¿Qué puede ocurrir si tras haber instalado todas las aplicaciones y al conectar mi token cryptoKEY este no se ilumina con una luz verde?
Conecte el lector en otro puerto USB de otro ordenador. Si sigue sin funcionar, pruebe en otro ordenador. Si el LED verde nunca se ilumina, consulte con Izenpe para reemplazar el token cryptoKEY.

¿Cómo puedo comprobar que mi token cryptoKEY lleva incorporada una tarjeta inteligente tamaño SIM en su interior?
Abra la pestaña que se encuentra en el lado puerto al conector USB y verifique, según la foto adjunto, que tiene una tarjeta inteligente tamaño SIM en su interior, insertada correctamente.



¿Qué puede ocurrir si al intentar cambiar el PIN de la tarjeta le aparece me el mensaje de error "C_SetPIN debido al error 0x6"?
Compruebe que el nuevo PIN tiene entre 6 y 8 dígitos alfanuméricos.

¿Puedo combinar números y letras para el número PIN de la tarjeta?
Sí, no hay ningún problema, siempre que el nuevo PIN tenga entre 6 y 8 dígitos.

¿Existe un máximo de inserciones de PIN en el caso de que tenga alguna duda y no recuerde mi número PIN? ¿Cuándo puede quedar bloqueada la tarjeta?
Si inserta más de 3 veces el código PIN de forma errónea, este se bloquea. Póngase en contacto con Izenpe para desbloquearlo.

¿Existe un máximo de inserciones de PUK para intentar desbloquear el PIN? ¿Qué ocurre si la tarjeta queda bloqueada?
Si inserta más de 3 veces el código PUK de forma errónea, este se bloquea. Por razones de seguridad, la tarjeta se bloquea completamente. Póngase en contacto con Izenpe.

¿Cómo puedo comprobar que dispongo de las últimas versiones del Kit Izenpe?

Puede comprobar la versión instalada de forma sencilla. En Windows XP, diríjase al menú Inicio > Programas > Izenpe > Desinstalar Kit Izenpe x.x.x.x (dónde x.x.x.x representa el número de versión instalada).

En Windows Vista o 7, diríjase al menú Inicio > Todos los programas > Izenpe > Desinstalar Kit Izenpe x.x.x.x (dónde x.x.x.x representa el número de versión instalada).

En Windows 8 diríjase a la pantalla de Inicio y haga click con el botón derecho. Le aparecerá un icono con el nombre "Todas las aplicaciones". Púlselo y busque la aplicación de Izenpe > Desinstalar Kit Izenpe x.x.x.x (dónde x.x.x.x representa el número de versión instalada).

Compruebe en el sitio web de Izenpe que corresponde con la última versión.

¿Qué puede ocurrir si al ejecutar el instalador del Kit_Izenpe User tengo una versión anterior instalada en el ordenador?

Siempre es recomendable eliminar versiones anteriores antes de instalar. No obstante, el instalador está diseñado para detectarlo automáticamente y eliminar versiones anteriores. Siga atentamente las instrucciones por pantalla.

Glosario

Autoridad de Certificación: Es la entidad de confianza, responsable de emitir y revocar los certificados electrónicos, utilizados en la firma electrónica. La Autoridad de Certificación, por sí misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad.

Caducidad del certificado digital: El certificado digital tiene un período de vigencia que consta en el mismo certificado. Generalmente es de 2 años, aunque por ley se permite una vigencia de hasta 5 años. Una vez el certificado haya caducado, no se podrán utilizar los servicios ofrecidos por la Administración que requieran firma electrónica, y cualquier firma electrónica que se haga a partir de ese momento no tendrá validez.

Certificado digital: Documento en soporte informático emitido y firmado por la Autoridad de Certificación, que garantiza la identidad de su propietario.

Certificado reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Firma electrónica: Conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. Existen 3 tipos de firma electrónica: firma electrónica simple, avanzada y reconocida.

Firma electrónica simple: Conjunto de datos, en forma electrónica, anejos a otros datos.

Firma electrónica avanzada: Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Firma electrónica reconocida: Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

Hash o Huella digital: Resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

Integridad: La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

Listas de Revocación de Certificados o Listas de Certificados Revocados: Lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

No repudio: El emisor que firme electrónicamente un documento no podrá negar que envió el mensaje original, ya que éste es imputable al emisor por medio de la clave privada que únicamente conoce él y que está obligado a custodiar. El no repudio permite, además, comprobar quién participó en una transacción.

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero

Prestador de Servicios de Certificación o PSC: Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Ver Autoridad de Certificación.

PIN: Secuencia de caracteres que permiten el acceso a los certificados. Número de Identificación Personal, en ocasiones llamado NIP.

PUK: Secuencia de caracteres que permiten el cambio o desbloqueo del PIN. Clave Personal de Desbloqueo.

Renovación: La renovación consiste en solicitar un nuevo certificado mediante un certificado vigente pero que está a punto de caducar. De esta manera, antes de la caducidad de un certificado se puede solicitar la renovación y esto implica que se emita un nuevo certificado válido.

Revocación: Anulación definitiva de un certificado digital a petición del suscriptor, o por propia iniciativa de la Autoridad de Certificación en caso de duda de la seguridad de las claves. La revocación es un estado irreversible. Se puede solicitar la revocación de un certificado después de una situación de suspensión o por voluntad de las personas autorizadas a solicitarla. De la misma manera, en el caso de un certificado suspendido, si ha pasado el periodo de suspensión máximo, si el certificado no ha sido habilitado, pasa a estar definitivamente revocado. Cuando la entidad de certificación revoca o suspende un certificado, ha de hacerlo constar en las Listas de Certificados Revocados (CRL), para hacer público este hecho. Estas listas son públicas y deben estar siempre disponibles.

Tarjeta inteligente (smartcard): Cualquier tarjeta con circuitos integrados que permiten la ejecución de cierta lógica programada.